Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 03 June 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports a communications outage at the New York Stock Exchange in the critical final minutes of trading on Wednesday, along with the exchange's refusal to detail what went wrong, frustrated customers and exposed frailties of the electronic system. (See item 6)
- CNET News reports the Anti−Phishing Working Group is coordinating efforts to build a central repository for phishing data, to protect Internet users and help catch cybercriminals. (See item 8)
- The New Scientist reports amid ominous signs that H5N1 bird flu is acquiring the ability to spread more readily among people, many health authorities are pinning their hopes on Tamiflu, the only available antiviral drug known to block the replication of the virus. (See item 19)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 02, Reuters* — **Russian oil output stagnant for eighth month.** Russian oil output rose 30,000 barrels per day (bpd) in May from April to 9.33 million bpd, but remained below a post−Soviet high recorded last year, the Energy Ministry's data showed on Thursday, June 2. The figures extend for an eighth consecutive month a period of stagnation in Russia's oil output.

Having risen to the new post−Soviet high of 9.42 million bpd last September, production has since fallen due to seasonal factors, the YUKOS oil company crisis, and higher taxes. Analysts have said the slowdown in output is further confirmation that the Kremlin's breakup of YUKOS and high taxation has sapped the Russian oil industry's ability to respond to booming global demand and record prices. Last week, Russia's Economy Ministry cut its 2005 gross domestic product growth forecast to 5.8 percent from 6.5 percent, citing slower oil growth as the main reason. Russian oil production has risen more than 50 percent since 1999, prompting President Vladimir Putin to set an ambitious goal of doubling the size of the economy by next decade, a target which many analysts say is now almost not feasible. Russia is the world's second largest oil exporter.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/02/AR2005060200250.html

2. *June 02, Reuters* — **Backup supplies for attacks looked at for electric transmission system.** Because of the near impossibility of guarding the entire U.S. electrical grid, industry representatives and government officials have shifted strategy in a bid to minimize disruptions from prolonged power outages. They are aiming to stockpile supplies of transformers, switches, generators and other gear to rush to a damaged station to speed up power restoration in the event of an emergency. The loss of the big transformers alone that adjust power voltage on transmission lines could prolong regional blackouts for months, energy analysts say. "Spares are in critical supply. The equipment is not easy to come by," said Joanne Callahan, a spokesperson for the North American Electric Reliability Council, or NERC, an industry group that sets operating rules for the grid. Analysts say it is probably not possible to erect physical barriers around all the pieces that make up the electricity system −− thousands of power plants, more than 637,000 miles of transmission lines and towers, substations and local neighborhood distribution lines. The program is building a database of supplies, but there is no industry−wide stockpile currently available.
Source: http://abcnews.go.com/US/wireStory?id=813280

3. *June 01, Nuclear Regulatory Commission* — **Nuclear Regulatory Commission revises regulations on access to classified information.** The Nuclear Regulatory Commission (NRC) is revising its regulations to expand the categories of persons who may seek access to classified information associated with NRC−regulated activities, as well as the categories of facilities that may be authorized to store such information. The revisions will allow the agency to process any requests for security clearances from (1) potential intervenors in a hearing for a potential high−level radioactive waste repository and (2) advanced reactor design vendors. The amendments also extend the regulations on facility security clearances. Current regulations permit persons and companies associated with NRC−regulated reactors, fuel cycle facilities and independent spent fuel storage installations to seek a facility security clearance to use, store, reproduce, transmit, transport or handle NRC classified information. The changes allow persons associated with other activities designated by the Commission (such as advanced reactor design vendors) to apply for a facility security clearance. The effective date will be July 5, 2005.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2005/05−0 87.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *June 02, ZDNet Australia* — **Trojan horse could be used for recruitment into criminal activity.** A recent malware attack in which a Trojan encrypts a user's files until the victim pays a US$200 ransom, could help criminal groups recruit people into money laundering and other dirty work, according to security experts. According to an advisory published by research group Gartner, this type of attack could evolve to a state where criminal groups blackmail their victims into performing dirty work in order to decrypt their files. According to the advisory, criminal groups will find receiving a cash ransom difficult because it would leave a money trail, so they are likely to try and use their victims to help other areas of their business. "Thieves will find it difficult to extract direct monetary payments for this type of attack, since such payments could be tracked. However, the threat of hostage data could also be used for other forms of extortion, with users compelled to perform dirty work to recover their files. Thieves could unlock the files gradually, drawing the users deeper into their schemes," the advisory said. Neil Campbell, national security manager of information technology services company Dimension Data, said that victims' could be persuaded into, for example, becoming a mule for diverting funds from phishing attacks.
   Source: http://www.zdnet.com.au/news/security/0,2000061744,39195013, 00.htm

5. *June 02, Associated Press* — **Small banks try token−based security.** Several small banks are launching heightened security programs this month to try to thwart identity theft and make customers feel more comfortable with online transactions. West Chester, PA−based Stonebridge Bank and Corpus Christi, TX−based American Bank are among the financial companies rolling out an optional program that relies on RSA Security Inc.'s strong authentication tokens, battery−powered devices that display a different six−digit password every 60 seconds. To conduct online transactions, the customer must enter the random number on the display, as well as a user name and password. So−called multi−factor authentication is common in Scandinavia, Brazil, and Singapore. In the United States, it's generally limited to employees accessing office networks remotely or people with high−value financial portfolios. However, with so many sites requiring passwords, many online shoppers and bankers have created simple passwords that are easy to guess. Fred Schea, chief financial officer of Stonebridge Bank, says the new program provides extra security without making customers remember another password. It also reduces risk for people who do their banking from laptops or public terminals at libraries, Internet cafes, or other sites frequented by hackers who sniff passwords.
   Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=163702992

6. *June 02, Reuters* — **Computer glitch halts trading at major exchanges.** A communications outage at the New York Stock Exchange (NYSE) in the critical final minutes of trading on Wednesday, June 1, and the exchange's refusal to immediately detail what went wrong frustrated customers and exposed frailties of its electronic systems. On Thursday, June 2, NYSE Chief Executive John Thain said that the problem occurred when the exchange's computer system and its backup were overwhelmed by an error message that duplicated millions of times. The exchange has taken steps to correct the problem and it shouldn't happen again, Thain said. Still, Thain on May 12 had told a Reuters Summit that the exchange relies on a communications system that "can tolerate multiple faults across the system." The glitch on Wednesday prompted the NYSE to halt floor trading four minutes before the scheduled 4 p.m. close, which is a time when many customers rush to fill orders. The glitch was related to the Securities Industry Automation Corp., or SIAC, an electronic system that disseminates market data and runs computer trading systems. Robert Morris, director of equity investments at Lord, Abbett & Co., said that NYSE rival Nasdaq has had similar trading disruptions. Trade at the American Stock Exchange was also disrupted.
Source: http://www.nytimes.com/reuters/business/business−markets−nys e−trading.html

7. *June 01, Agence France−Presse* — **Internet scammers make simultaneous attack on French banks.** Four major French banks have issued warnings to their clients after Internet scammers made a simultaneous attempt to gain access to confidential customer information, a bank spokesperson said Wednesday, June 1. BNP Paribas, Societe Generale, CCF and CIC all issued warnings to their clients via their Websites after the massive attempted fraud on Friday, May 27, which police are investigating. The fraud involved an unsolicited or spam e−mail to potential bank clients which appeared to come from a bank and which asked for confirmation of confidential account details on the bank's Internet site, which was a fake copy. There was now a risk that the scammers would attempt a second more targeted scam with the client information they collected from the first attempt, said a bank spokesperson. What was new in this attempted scam was that it targeted, in the same e−mail message, the huge number of potential bank clients of four banks at the same time, said the spokesperson. It is not known how many customers responded to the scam.
Source: http://www.menafn.com/qn_news_story.asp?StoryId=CqP0YWeienJC 3nuLUDgvYBMv0zNjHDwrZD

8. *June 01, CNET News* — **Group pools data to trap phishers.** The Anti−Phishing Working Group is coordinating efforts to build a central repository for phishing data, to better protect Internet users and help catch cybercriminals. The group has expanded its simple list of phishing scams into a database that can be used for analyses and to share information with members, said Patrick Cain, a research fellow at the group. Additionally, a standard XML, or extensible markup language, form has been created to facilitate the submission of data on attacks to the organization, he said. "We're hoping to become a clearinghouse" for phishing data, Cain said. The data could be used in products to protect Internet users and for analyses of attacks, which in turn could help law enforcement track down phishers, Cain said. The group's list already includes data on about 75,000 phishing e−mails, he said. The Anti−Phishing Working Group was established last year to combat fraud and identity theft resulting from phishing and related attacks. The group's members include banks, Internet service providers, law enforcement agencies and technology vendors.
Anti−PhishingWorking Group: http://www.antiphishing.org/index.html

Source: http://news.zdnet.com/2100−1009_22−5728622.html

[Return to top]

Transportation and Border Security Sector

9. *June 02, Washington Post* — **District plans river ferry experiment.** Washington, DC's Department of Transportation has begun considering several proposals for a commuter ferry service on the Potomac and Anacostia rivers and hopes to have a vessel on the water by next spring, officials said. At least four companies have expressed interest in securing the $500,000 contract for an 18−month pilot program that would run a water coach or ferry serving commuters in the mornings and evenings and tourists during the day. Plans to tap the unrealized potential of the Potomac as a commuter route have been around for decades, but past efforts to get a ferry running have fizzled under financial pressure. Proponents of the new plan say the time is ripe, as the area's traffic−clogged highways have made it the third−most congested region in the country. Though other U.S. cities −− such as New York, San Francisco and Seattle −− have thriving ferry systems for commuters, the District has so far seen only feasibility studies, going as far back as 1964. In 1999, a Virginia Department of Transportation study found that a 45−minute ferry commuter service from Woodbridge to the Navy Yard could work −− at about the cost of a commuter rail trip.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/01/AR2005060101699.html?sub=AR

10. *June 02, Indianapolis Star* — **ATA seeks interim backing.** ATA Airlines will look for a new cash infusion from investors to help carry it through the lean months expected before profits rise next spring. "We're looking at our business plan and think we need a few more dollars to help us going forward," John Denison, ATA chief executive, said Wednesday, June 1. It was the first public indication the 5,700−employee airline might turn to hedge funds or other investors for operating capital. The bankrupt Indianapolis carrier is running through a $40 million loan from business partner Southwest Airlines of Dallas and needs a capital infusion to keep going. Air Line Pilots Association members currently are voting on temporary 18% wage concessions that would expire in August. In addition to the concessions, Denison said the airline is trying to figure just how much cash it would need to raise from investors such as a hedge fund. ATA reported Wednesday it lost $12.63 million in April on operating revenue of $87.11 million. Operating expenses totaled $98.18 million, including $25.6 million for fuel and $23 million for payroll. Reorganization expenses totaled $1.18 million. Indianapolis−based ATA Holdings Corp. and its various units, including ATA Airlines, filed for Chapter 11 bankruptcy on October 26.
Source: http://www.usatoday.com/travel/news/2005−06−02−ata−loans_x.h tm

11. *June 02, NorthJersey.com* — **Port Authority chief would cut Teterboro air traffic.** Flights to and from New Jersey's Teterboro airport should be reduced to enhance safety at the busy airport, the head of the Port Authority of New York and New Jersey said Wednesday, June 1. "If there is a way for us to create capacity in other locations where [Teterboro] can operate at levels that are safer, we should seriously consider that," said agency Chair Anthony Coscia, who nonetheless maintained that the airport is safe. The pilot of a twin−engine turboprop crashed on landing Tuesday, May 31, revving up critics and elected officials who renewed calls

to reduce activity at the airport, which logged more than 200,000 takeoffs and landings last year. Talk of limiting flights has always been a touchy subject within the aviation community. The Federal Aviation Administration says that any airport receiving federal funding cannot unfairly limit air traffic. But after Tuesday's crash, elected officials began calling for reductions in flights by as much as 25 percent, a move that would require much more than simple noise restrictions. Coscia said it was premature for him to say how much or what kind of traffic should be reduced at Teterboro. Much of Teterboro's appeal to corporate and charter jets is its proximity to Manhattan and northern New Jersey corporations.
Source: http://www.bergen.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXkzJmZnYmVsN2Y3dnFlZUVFeXk2NzAyNjIzJnlyaXJ5N2Y3MTdmN3ZxZWVFRXl5Mw==

12. *June 02, Department of Transportation* — **FAA investigation into New York TRACON.** A 60−day on−site investigation of the New York Terminal Radar Approach Control (TRACON) facility found that it is more than adequately staffed for safe operations and that local union−controlled scheduling practices are inefficient and wasteful, creating overtime costs that are more than double any other air traffic control facility in the country. The investigation also found recent management attempts to curb wasteful practices were met with resistance, followed by anonymous reports of “operational errors.” As a result of the investigation's findings, the Department of Transportation’s Federal Aviation Administration (FAA) is immediately acting to curb scheduling abuses that drive excessive overtime spending, address reports of intimidation and insubordination, and ensure controllers' adherence to existing high safety standards. On March 2, 2005, the FAA assembled a team of over 25 safety experts from around the country, including current and former air traffic controllers, current field supervisors, and human resource and organizational professionals to conduct an onsite operational assessment of the New York TRACON. The team conducted a thorough audit of radar and voice data, facility scheduling practices, shift assignments, controller time−on−position, and overtime and leave usage. The team's audit also consisted of dozens of interviews with managers, supervisors, and employees and first−hand observation of control room operations.
FAA report: http://www.faa.gov/library/reports/
Source: http://www.dot.gov/affairs/faa060205.htm

13. *June 01, Associated Press* — **U.S., Mexico to continue repatriation program.** Illegal immigrants caught crossing the Mexican border will be offered a free ticket home in the second summer of an experimental Department of Homeland Security program, U.S. and Mexico officials said Tuesday, May 31. The so−called repatriation program aims to reduce the chances of migrants re−crossing the porous Arizona border by flying them deep into the interior of Mexico. But immigrants rights groups charge the program is expensive and ineffective. Mexico Interior Minister Santiago Creel told reporters in Washington that last year's program "gave us satisfactory results." Over a three−month period last summer, at a cost of $15.4 million, U.S. Customs and Border Protection captured 14,067 illegal border crossers and flew them to Mexico City and Guadalajara. From there, the migrants were given bus tickets to their home communities. Currently, illegal immigrants captured in the United States are flown or bused to the border. Department of Homeland Security Secretary Michael Chertoff said the program would resume shortly, but he said he did not know whether it would be an annual event.
Source: http://www.dhonline.com/articles/2005/06/02/news/nation/nat0 3.txt

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *June 02, StopSoybeanRust.com* — **More soybean rust found in two Georgia counties.** Georgia soybean specialists believe they've found evidence of Asian soybean rust on volunteer soybeans again −– in a new spot four miles from the original Seminole County discovery, and possibly in another field in Terrell County, four counties to the north. Bob Kemerait, plant pathologist with the University of Georgia Extension Service, told StopSoybeanRust.com that while he and a group of students were destroying the original patch of infected soybeans near Donalsonville on May 26, a county agent went to another site and brought back volunteer soybeans and kudzu that looked suspicious. There were sparse sporulations on the volunteer soybeans from what they call the "Hanna site" in Seminole County, Kemerait said, but under the microscope, "they were beautiful spores." They were identical to those he confirmed as Asian soybean rust back on April 27, he said. Also on May 26, scouts were rechecking a site in Terrell County near where they suspected rust in April, but couldn't go back for more samples of the rusty−looking volunteer beans because they were harrowed under before enough spores could be collected to run tests and confirm the sighting. This time, they found more volunteer soybean, some "in a location near some barns where they had been transferring soybean seed last year at harvest," Kemerait said. "We have some more suspicious spores." Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=337

15. *June 02, Xinhuanet* — **Japan confirms 19th case of mad cow disease.** A nine−year−old Holstein cow in Hokkaido, Japan, was diagnosed with the 19th case of mad cow disease in Japan, the Japanese Ministry of Health, Labor and Welfare said Thursday, June 2. The cow was born in the spring of 1996, which was around the same time as many other cows infected with the disease called bovine spongiform encephalopathy were born. As the cow was born before feeding cows with meat−and−bone meal was banned in 2001 due to fear of infection by the disease, the ministry said that latest case did not change its current anti−BSE measures. Source: http://news.xinhuanet.com/english/2005−06/02/content_3037455 .htm

[Return to top]

Food Sector

16. *June 01, Business Journal of Phoenix (AZ)* — **CHS sells tortilla and chip production facilities.** CHS Inc., completed the sale of its tortilla and chip operations in Phoenix, AZ, and other cities to Gruma Corp., a Mexican corn miller and tortilla maker, CHS officials said Wednesday, June 1. In addition to the Phoenix plant, plants located in New Brighton, MN, and Fort Worth, TX, were also sold. Gruma markets its finished products under the Mission and

Guerrero names. CHS Inc., is a Minnesota−based diversified energy, grains and foods company.
Source: http://phoenix.bizjournals.com/phoenix/stories/2005/05/30/da ily24.html

17. *June 01, Reuters* — **Japan finds biotech corn, will test all U.S. imports.** Japan, the biggest buyer of U.S. corn, found an American shipment tainted with the unapproved Bt−10 biotech variety and will begin testing every U.S. cargo, a Japanese official told Reuters on Wednesday, June 1. The official confirmed that Thursday, May 26, a 390 ton shipment to Japan from the U.S. was found to contain Bt−10. Bt−10 corn, manufactured by Swiss agrochemicals group Syngenta AG, is engineered to resist the corn borer insect. It was accidentally mixed with U.S. grain shipments between 2001 and 2004. Last month, the Japanese government began spot−testing some U.S. cargoes for Bt−10 corn. Japan has a zero tolerance policy on imports of unapproved biotech foods. Japan buys about 16 million ton of corn annually, with 90 percent of it from the U.S.
Source: http://www.planetark.com/dailynewsstory.cfm/newsid/31062/sto ry.htm

[Return to top]

Water Sector

18. *June 02, Federal Energy Regulatory Commission* — **Sinkhole near Swinging Bridge Dam in New York.** On May 5, a “sinkhole” was discovered in the crest of the Swinging Bridge Dam in New York state. An investigative program commenced to assess the condition of the dam, to determine the cause of the sinkhole, and to determine actions necessary to correct the problem. The Federal Energy Regulatory Commission has required the licensee, Mirant NY to retain the services of a Board of Consultants to oversee investigations and the design and the construction of remedial measures needed to correct the deficiency. With the urgency of the situation and concern for dam safety the reservoir has been drawn down to a safe level. The sinkhole has been backfilled with sand and gravel. No further movements, displacements, or anomalies have been observed during this period of enhanced monitoring and surveillance established at the site. Therefore, the situation appears to have been stabilized.
Source: http://www.ferc.gov/industries/hydropower/safety/swinging.as p

[Return to top]

Public Health Sector

19. *June 02, New Scientist* — **Tamiflu possible bird flu treatment.** Amid ominous signs that H5N1 bird flu is acquiring the ability to spread more readily among people, many health authorities are pinning their hopes on Tamiflu, the only available antiviral drug known to block the replication of the virus. Even if efforts to develop a vaccine are successful, it could take many months to produce the billions of doses needed in the event of a pandemic. By then it might be too late. So in the meantime, the World Health Organization is stepping up its efforts to acquire a massive stockpile of Tamiflu, which it hopes will at least slow any emerging flu pandemic. Tamiflu can save lives if it is given early, no more than two days after symptoms first appear. Ira Longini, of Emory University, says much depends on how fast the virus

spreads. If each infected person passes the virus to fewer than two other people on average, then isolating and treating all cases and their contacts with antivirals could slow or even stop an epidemic, he calculates. But health workers would not be able to keep up with the virus if sick people infect between two and three others. Drug stockpiles would still help save lives, Longini says, but would not halt the outbreak.
Source: http://www.newscientist.com/article.ns?id=mg18625023.100

20. *June 01, National Institute of Allergy and Infectious Diseases* — **New grants for biodefense and infectious diseases research network.** The National Institute of Allergy and Infectious Diseases (NIAID), part of the National Institutes of Health, Wednesday, June 1, announced four−year grants totaling approximately $80 million for two new Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases Research (RCE). The grants to the University of California, Irvine, and Colorado State University mark the completion of a national network of academic centers that conducts research to counter threats from bioterror agents and emerging infectious diseases. Each institution will receive approximately $10 million per year for the next four years to head a regional research consortium. NIAID established the RCE network in 2003 with grants to eight institutions. Each institution also leads an RCE consortium made up of universities and other research institutions within its geographic region. The network conducts research that will lead to next−generation treatments, vaccines, and diagnostic tools for diseases such as anthrax, plague, smallpox, tularemia, botulism, and West Nile fever. University of California, Irvine, will head a consortium whose members include four additional University of California campuses and 11 other regional universities and research institutions. Colorado State University will head a consortium whose members include five other universities plus small business partners; it also includes substantial collaboration with the Centers for Disease Control and Prevention.
Source: http://www2.niaid.nih.gov/newsroom/Releases/rce_05.htm

[Return to top]

Government Sector

21. *June 01, Federal Computer Week* — **DHS improving information−sharing capabilities.** The Department of Homeland Security (DHS) is slowly improving its information−sharing capabilities, a DHS official said Wednesday, June 1. "We're basically on the right track, but it will be a while before we do everything that needs to be done," said Martin Smith, program manager for information technology information sharing in the Department of Homeland Security's Office of the Chief Information Officer. DHS is creating a nationwide network for sharing sensitive information and getting the right information to the right people in time for them to take effective action, Smith said. DHS has taken a number of steps to improve information sharing, he added. In addition to creating the Information Sharing and Collaboration Office, it has brought together project managers from most of its directorates and agencies to create a "core of people with cross−cutting knowledge of the department," Smith said. Their mandate is to improve information sharing and prevent the stove piping of information, he said.
Source: http://www.fcw.com/article89031−06−01−05−Web

[Return to top]

Emergency Services Sector

22. *June 02, SDSUniverse (CA)* — **Simulated bomb blast to test San Diego's disaster preparedness.** Emergency responders from all over San Diego, CA, will converge on campus Monday, June 6, for a full−scale emergency response drill in the San Diego State University (SDSU) trolley station. The drill will begin shortly after 9 a.m., with the simulation of a bomb blast on a trolley in the new underground station. Emergency responders from SDSU Public Safety, the San Diego Police and Fire departments, the La Mesa Police Department, the California Highway Patrol, the California Department of Transportation, and the California State Fire Marshal will participate in the two−hour exercise. Also taking part are representatives from the County of San Diego Emergency Preparedness unit. This is the latest in a series of emergency drills conducted by the Metropolitan Transit System and funded by a $150,000 grant from the Federal Transit Administration to support enhanced multi−jurisdictional emergency preparedness training. Nearly 100 law enforcement officers will operate out of parking lot G during the simulation.
Source: http://www.sdsuniverse.info/story.asp?id=30937

23. *June 02, Government Technology* — **Virginia announces online toolkit to help businesses prepare for disasters.** On Wednesday, June 1, Virginia Governor Mark R. Warner announced a new, online resource designed to help Virginia businesses prepare for and recover from disasters. The Virginia Business Emergency Survival Toolkit features information and resources to help businesses prevent and reduce disaster−related losses. In the last six years alone, natural disasters have caused billions of dollars in structural damages and lost revenue for Virginia businesses. June 1 marks the first day of the Atlantic hurricane season. Hurricanes, tropical storms, and floods have affected large portions of Virginia. The online toolkit outlines simple measures businesses can take now to prepare for emergencies. It covers all areas of business emergency planning, including identifying hazards and threats, preparing employees, developing disaster plans, covering insurance needs, responding to an emergency, and arranging recovery assistance. Companies that already have emergency plans in place should review their plans to ensure they are up to date. The Virginia Business Emergency Survival Toolkit was developed by Virginia Citizen Corps, the Virginia Department of Emergency Management, the Virginia Department of Business Assistance, the Virginia Crime Prevention Association, the American Red Cross and representatives from several of Virginia's chambers of commerce.
Toolkit: http://www.vaemergency.com/business
Source: http://www.govtech.net/news/news.php?id=94155

24. *June 02, Associated Press* — **Kansas takes steps toward upgraded communications system.** State officials unveiled an initiative Wednesday, June 1, to create a seamless communications system for first responders and emergency management agencies across Kansas. Financed by $16 million in federal grants and state transportation funds, the project will open 76 Kansas Department of Transportation (KDOT) towers to local government agencies and help upgrade communications systems for 17 southeast Kansas counties. The goal is to link police, fire, ambulance and other first responders during emergencies. The project is the first step in an initiative created by 2004 legislation. Legislators saw a need for effective communication links after the September 11 terror attacks. Emergency management officials said they have faced

problems for years in responding to calls. Col. William Seck, the Highway Patrol's superintendent, said communication difficulties are cited in every briefing after an emergency. Use of different codes and language by agencies and myriad radio systems and capabilities hamper effective responses when lives and property are at risk, he said. Using KDOT towers and additional communication systems will help link agencies regardless of the frequencies they use, he said.
Source: http://www.officer.com/article/article.jsp?siteSection=6&id= 24001

[Return to top]

Information Technology and Telecommunications Sector

25. *June 02, Reuters* — **Sun Micro to buy StorageTek for $4.1 billion.** Network computer maker Sun Microsystems Inc. said on Thursday, June 2, it had agreed to buy Storage Technology Corp. for $4.1 billion in cash, bolstering its presence in the fast−growing market for data storage. California−based Sun will pay $37 per share for Colorado−based Storage Technology, also known as StorageTek. Sun's CEO Scott McNealy said that, with increased regulations on companies regarding compliance issues in financial services and increased data requirements in health care, the transaction made sense. "It was becoming a more and more important component of solving these complex network computing problems," McNealy said, referring to data storage issues facing companies.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/02/AR2005060200518.html

26. *June 01, SecurityFocus* — **Symantec Brightmail AntiSpam remote information disclosure vulnerability.** Symantec Brightmail AntiSpam is susceptible to a remote information disclosure vulnerability. This issue is due to a failure of the application to properly ensure that remote database access is properly disabled. Original advisory and updates:
http://securityresponse.symantec.com/avcenter/security/Conte nt/2005.05.31a.html
Source: http://www.securityfocus.com/bid/13828

27. *June 01, SecurityFocus* — **NASM IEEE_PUTASCII remote buffer overflow vulnerability.** NASM is prone to a remote buffer overflow vulnerability. An attacker exploits this issue by crafting a malicious source file to be assembled by the application. This file is sent to an affected user and if the user loads the file in NASM, the attack may result in arbitrary code execution. The attacker may then gain unauthorized access in the context of the user running NASM. Refer to Source link below for vendor solutions.
Source: http://www.securityfocus.com/bid/13506

28. *June 01, SecurityFocus* — **Microsoft Outlook Express attachment processing file extension obfuscation vulnerability.** Microsoft Outlook Express is prone to an attachment file extension obfuscation vulnerability that may present a risk under certain configurations. Reports indicate that this may be leveraged to make the attached email message executable. It is possible to cause a default file handler to be invoked to process the attached email message and potentially allowing for code execution. This issue may lure a victim into a false sense of security and may result in inadvertent or unintentional execution of attacker supplied code. There is no solution at

this time.
Source: http://www.securityfocus.com/bid/13837/info

29. *June 01, IDG News Service* — **Study: U.S. Internet users at risk for online exploitation.** U.S. Internet users are dangerously ignorant about the type of data that Website owners collect from them and how that data is used, according to a new study by the University of Pennsylvania's Annenberg Public Policy Center. The lack of awareness makes U.S. Internet users vulnerable to online exploitation, such as misuse of personal information, fraud and overcharging, the study said. Titled "Open to Exploitation: American Shoppers Online and Offline," the study involved 1,500 adult U.S. Internet users who were asked true−or−false questions about topics such as Website privacy policies and retailers' pricing schemes. Respondents on average failed the test. According to the authors, some alarming findings include: seventy−five percent of respondents wrongly believe that if a Website has a privacy policy, it won't share their information with third parties and that almost half of the respondents couldn't identify "phishing" scam e−mail messages. To address the problems identified by the study, the authors proposed replacing the term "Privacy Policy" with "Using Your Information," teaching consumer education and media literacy taught in elementary, middle and high schools in the U.S., and requiring online retailers to disclose what data they have collected about customers.
Study: http://www.annenbergpublicpolicycenter.org/04_info_society/Turow_%20APPC_Press_Release_WEB_FINAL.pdf
Source: http://www.computerworld.com/securitytopics/security/story/0,10801,102155,00.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports a heap−based buffer overflow that affects the PHP 'pack()' function call. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to execute arbitrary instructions in the context of the vulnerable process. This function allows a malicious programmer to set references to entries of a variable hash that have already been freed. This can lead to remote memory corruption and may allow them to gain access to potentially sensitive information, such as database credentials.

Current Port Attacks

Top 10 Target Ports	135 (epmap), 445 (microsoft−ds), 1026 (−−−), 1027 (icq), 1433 (ms−sql−s), 1434 (ms−sql−m), 4899 (radmin), 139 (netbios−ssn), 1028 (−−−), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center)

Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.